UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00052

ZERO-CLICK KERNEL BUG IN LINUX IOT DEVICES

DATE ISSUED: 20th October 2020

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Versions of the Linux kernel prior to version 5.9 that support BlueZ, the core Bluetooth protocol stack, are vulnerable to a high-severity flaw, and two lesser bugs in Linux-based Internet of Things (IoT) devices, that are all caused by deficient authentication and access control. CVE-2020-12351, CVE-2020-12352, CVE-2020-24490

BREAKDOWN

Google has dubbed the flaw "BleedingTooth" which may be exploited using bespoke input by any local, unauthenticated attacker and has the potential to leave to privilege escalation in any affected devices. Although this stack has not been a part of the official Linux kernel since version 2.4.6, it is still currently in use in some Bluetooth devices. Because Bluetooth is a close proximity method of transmission, the attacker must be near to the device and be aware oof its bd address. If this is known, a Logical Link Control and Adaptation Layer (l2cap) packet may be transmitted, causing Denial of Service (DoS) or code execution on the device as well as potential data leak or losses. This vulnerability is classified as a type-confusion vulnerability and in this case, the issues stem from inadequate validation of user input in BlueZ. Further flaws may be exploited to undertake retrieval of the kernel stack to discover memory mapping and retrieve desirable information such as encryption keys.

REMEDIATION STEPS

- Update any Linux-based IoT devices using the BlueZ protocol stack to version 5.9 or higher
- Disable Bluetooth on any devices when not in use

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/google-intel-kernel-bug-linux-iot/160067/
Security Week	https://www.securityweek.com/bleedingtooth-vulnerabilities-linux-bluetooth-allow-zero-click-attacks
ZDNet	https://www.zdnet.com/article/google-warns-of-severe-bleedingtooth-bluetooth-flaw-in-linux-kernel/
The Hacker News	https://thehackernews.com/2020/10/linux-Bluetooth-hacking.html